



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/666,519	09/20/2000	Alexander G. Dickinson	48556.00001	6942
23767	7590	09/16/2005	EXAMINER	
PRESTON GATES ELLIS & ROUVELAS MEEDS LLP 1735 NEW YORK AVENUE, NW, SUITE 500 WASHINGTON, DC 20006			HA, LEYNNA A	
			ART UNIT	PAPER NUMBER
			2135	

DATE MAILED: 09/16/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)
	09/666,519	DICKINSON ET AL.
	Examiner	Art Unit
	LEYNNA T. HA	2135

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) Responsive to communication(s) filed on September 9, 2004.
- 2a) This action is FINAL. 2b) This action is non-final.
- 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) Claim(s) 1-74 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) Claim(s) _____ is/are allowed.
- 6) Claim(s) 1-74 is/are rejected.
- 7) Claim(s) _____ is/are objected to.
- 8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) The specification is objected to by the Examiner.
- 10) The drawing(s) filed on _____ is/are: a) accepted or b) objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) All b) Some * c) None of:
1. Certified copies of the priority documents have been received.
2. Certified copies of the priority documents have been received in Application No. _____.
3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|---|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____. |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____. | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| | 6) <input type="checkbox"/> Other: _____. |

DETAILED ACTION

1. Applicant brought to attention that claims 70-74 were not addressed in the Final rejection mailed on 3/25/2005. The examiner inadvertently missed new claims 70-74 of applicant's 9/9/2004 response. Therefore, the period for this Final rejection has been restarted.

2. Claims 1-74 are pending.

3. Examiner's response to arguments.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. Claims 1-9, 54-58, and 70-74 are rejected under 35 U.S.C. 102(e) as being anticipated by BORZA (US 5,995,630).

As per claim 1:

BORZA discloses a remotely accessible secure cryptographic system for storing a plurality of private cryptographic keys to be associated with a plurality of users, wherein the cryptographic system associates each of the plurality of users with one or more different keys from the plurality of private cryptographic keys and performs cryptographic functions for each user using the associated one or more different keys without releasing the plurality of private cryptographic keys to the users, the cryptographic system comprising:

[see COL.6, line 1...Et. SEQ.]

a depository system having at least one server which stores a plurality of private cryptographic keys and a plurality of enrollment authentication data **[COL.8, lines 33-40]**, wherein each enrollment authentication data identifies one of multiple users **[COL.7, lines 5-11]** and each of the multiple users is associated with one or more different keys from the plurality of private cryptographic keys; **[COL.6, lines 29-30 and COL.8, lines 60-62]**

an authentication engine which compares authentication data received by one of the multiple users **[COL.6, lines 31-34]** and received from the depository system, thereby producing an authentication result; **[COL.6, lines 35-36 and COL.8, lines 48-53]**

a cryptographic engine which, when the authentication result indicates proper identification of the one of the multiple users **[COL.8, line 52]**, performs cryptographic functions on behalf of the one of the multiple users using the

associated one or more different keys received from the depository system; and
[COL.6, lines 36-38 and COL.8, lines 54-59]

a transaction engine connected to route data from the multiple users to the depository server system, the authentication engine, and the cryptographic engine. **[COL.8, lines 31-37 and COL.9, lines 17-50]**

As per claim 2:

BORZA discloses a remotely accessible secure cryptographic system comprising:

a depository system having at least one server which stores at least one private key and a plurality of enrollment authentication data **[COL.8, lines 33-40]**, wherein each enrollment authentication data identifies one of multiple users; **[COL.7, lines 5-11]**

an authentication engine which compares authentication data received by one of the multiple users **[COL.6, lines 31-36]** and received from the depository system, thereby producing an authentication result; **[COL.8, lines 48-53]**

a cryptographic engine which, when the authentication result indicates proper identification of the one of the multiple users **[COL.8, line 52]**, performs cryptographic functions on behalf of the one of the multiple users using the associated one or more different keys received from the depository system; and
[COL.6, lines 36-38 and COL.8, lines 54-59]

a transaction engine connected to route data from the multiple users to the depository server system, the authentication engine, and the cryptographic engine. **[COL.8, lines 31-37 and COL.9, lines 17-50]**

As per claim 3: See COL.6, lines 29-33 and COL.8, lines 34-36; discussing a plurality of storage facilities for storing the private key and the enrollment authentication data.

As per claim 4: See COL.7, lines 8-14 and COL.8, line 64 thru COL.9, line 3; discussing each substantially randomized portion is individually undecipherable.

As per claim 5: See COL.6, line 13; discussing the enrollment authentication data includes biometric data.

As per claim 6: See COL.6, lines 15-16; discussing the enrollment authentication data includes finger print patterns.

As per claim 7: See COL.5, line 66 and COL.8, lines 38-42, discussing the private key corresponding to the secure cryptographic system.

As per claim 8: See COL.8, lines 60-62; discussing at least one private key corresponding to one of the multiple users.

As per claim 9: See COL.8, lines 35-36, discussing cryptographic functions comprise one of digital signing, encryption, and decryption.

As per claim 54:

BORZA teaches the method of handling sensitive data in a cryptographic system, wherein the sensitive data exists in a useable form only during actions employing the sensitive data, the method comprising:

receiving in a software module, substantially randomized sensitive data from a first computer accessible storage medium; [COL.8, lines 48-51; the randomized sensitive data is the registered biometric data stored in the memory 123]

receiving in a software module, substantially randomized data from a second computer accessible storage medium; [COL.7, lines 30-38 and COL.8, lines 40-42; the fingerprint received from the imaging device and the algorithm specific (of the encryption/decryption circuit 124) for generating data from the image is the randomized data]

processing the substantially randomized sensitive data and the substantially randomized data in the software module to assemble the sensitive data; and [COL.8, lines 48-57; once the encode image (randomized data) and the registered biometric data is processed, a sensitive data key is assembled]

employing sensitive data in a software engine to perform an action, wherein the action includes one of authenticating a user and perform a cryptographic function. [COL.8, lines 57-67; once the user is authenticated, the key is given for encryption/decryption]

As per claim 55: See COL.9, lines 50-51; discusses destroying the sensitive data after completion of the action.

As per claim 56: See COL.6, lines 15-18; discussing biometric data cryptographic key data.

As per claim 57: See COL.6, lines 50-61; discussing at least one of the first and second computer accessible storage mediums comprise a secure server.

As per claim 58: See COL.7, lines 30-38; discussing authentication and cryptography.

As per claim 70:

BORZA teaches the method of handling sensitive data in a cryptographic system, wherein said sensitive data exists in a useable form only during actions employing said sensitive data, said method comprising:

receiving in a software module, substantially randomized sensitive data from a first computer accessible storage medium; [COL.8, lines 48-51; the randomized sensitive data is the registered biometric data stored in the memory 123]

receiving in said software module, substantially randomized data from a second computer accessible storage medium, processing said substantially randomized sensitive data and said substantially randomized data in said software module to assemble said sensitive data; and [COL.7, lines 30-38 and COL.8, lines 40-42; the fingerprint received from the imaging device and

the algorithm specific (of the encryption/decryption circuit 124) **for generating data from the image is the randomized data]**

employing said sensitive data in a software engine to perform a cryptographic function. **[COL.8, lines 57-67; once the user is authenticated, the key is given for encryption/decryption]**

As per claim 71: See COL.9, lines 50-51; discusses destroying said sensitive data after completion of said action.

As per claim 72: See COL.6, lines 15-18; discussing said sensitive data includes one of user biometric data and cryptographic key data.

As per claim 73: See COL.6, lines 50-61; discussing at least one of the first and second computer accessible storage mediums comprise a secure server.

As per claim 74: See COL.7, lines 30-38; discussing software module comprises a data assembling module and said software engine comprises one of an authentication engine and a cryptographic engine.

5. Claims 10-53 are rejected under 35 U.S.C. 102(e) as being anticipated by EPSTEIN. (US 6,453,416).

As per claim 10:

EPSTEIN teaches the method of facilitating cryptographic, the method comprising:

associating a user from multiple users with one or more keys from a plurality of private cryptographic keys [COL.4, lines 24-31] stored on a secure server; [COL.6, lines 28-55]

receiving authentication data from the user; [COL.4, lines 54-58]

comparing the authentication data to authentication data corresponding to the user, thereby verifying the identity of the user; and [COL.6, lines 20-38]

utilizing the one or more keys to perform cryptographic functions without releasing the one or more keys to the user. [COL.7, lines 26-48]

As per claim 11: See COL.6, lines 12-14, discussing the authentication data corresponding to the user was acquired prior to the step of receiving authentication data from the user.

As per claim 12: See COL.5, line 43 thru COL.6, line 67, for receiving the hash of a message or document.

As per claim 13: See COL.5, lines 63-66, discussing archiving the hash.

As per claim 14:

EPSTEIN discloses an authentication system for uniquely identifying a user through secure storage of the user's enrollment authentication data, the authentication system comprising:

a plurality of data storage facilities, wherein each data storage facility includes a computer accessible storage medium which stores one of portions of enrollment authentication data; and [COL.5, lines 63-66 and COL.6, lines 39-49]

an authentication engine which communicates with plurality of data storage facilities and comprises [COL.6, lines 12-30]

a data splitting module which operates on the enrollment authentication data to create portions, [COL.4, lines 53-58]

a data assembling module which processes the portions from at least two of the data storage facilities to assemble the enrollment authentication data, and [COL.6, lines 13-19]

data comparator module which receives current authentication data from a user and compares the current authentication data with the assembled enrollment authentication data to determine whether the user has been uniquely identified. [COL.6, lines 20-38]

As per claim 15: See COL.6, lines 12-14; discussing the portions are not individually decipherable.

As per claim 16: See COL.5, lines 63-66 and COL.6, lines 39-49; discussing each data storage facility is logically separated from any other data storage facility.

As per claim 17: See **COL.5, lines 63-66 [for the data storage within the smartcard] and COL.6, lines 39-49 [for the data storage within the server];** discussing each data storage facility is physically separated from any other data storage facility.

As per claim 18: See COL.6, lines 30-32; discusses a cryptographic engine which, upon the unique identification of the user by the authentication engine, provides cryptographic functionality to the user.

As per claim 19: See COL.6, lines 28-40; discussing the plurality of data storage facilities comprises at least one secure server.

As per claim 20: See COL.4, lines 24-29; discusses the unique identification of the user by the authentication engine provides the user authorization to gain access to or operate one or more systems.

As per claim 21: See COL.4, lines 47-48; discussing one or more electronic devices.

As per claim 22: See COL.5, lines 4-10; discussing computer software systems.

As per claim 23: See COL.4, lines 47-48; discussing one or more systems include one or more consumer electronic.

As per claim 24: See COL.4, lines 47-48; discussing one or more consumer electronics includes a cellular phone.

As per claim 25: See COL.4, lines 30-35; discussing one or more systems include one or more cryptographic systems.

As per claim 26: See COL.4, lines 47-52; discussing one or more systems include one or more physical locations.

As per claim 27: See COL.5, lines 63-66 and col.6, lines 39-49; discussing at least one of the data storage facilities stores at least some sensitive data, wherein the at least one of the data storage facilities serves the sensitive data when the authentication engine indicates that the user has been uniquely identified.

As per claim 28: See COL.5, lines 63-66 and col.6, lines 39-49; discussing a data vault which stores sensitive data, wherein the data vault serves the sensitive data when the authentication engine indicates that the user has been uniquely identified.

As per claim 29: See COL.6, lines 28-48 and COL.7, lines 9-14; discusses the identification system outputs an indication of whether the user has been uniquely identified.

As per claim 30:

EPSTEIN discloses a cryptographic system, comprising:

a plurality of data storage facilities, wherein each data storage facility includes a computer accessible storage medium which stores one of portions of cryptographic keys; and [COL.5, lines 63-66 and COL.6, lines 39-49]

a cryptographic engine which communicates with plurality of data storage facilities and comprises [COL.4, lines 30-35 and COL.6, lines 28-32]

a data splitting module which operates on the cryptographic keys to create portions, [COL.4, lines 53-58]

a data assembling module which processes the portions from at least two of the data storage facilities to assemble the cryptographic keys, and [COL.6, lines 13-19]

a cryptographic handling module which receives the assembled cryptographic keys and performs cryptographic functions therewith. [COL.6, lines 20-38]

As per claim 31: COL.6, lines 12-14; discussing the portions are not individually decipherable.

As per claim 32: See COL.5, lines 63-66 and COL.6, lines 39-49; discussing each data storage facility is logically separated from any other data storage facility.

As per claim 33: See COL.5, lines 63-66 [for the data storage within the smartcard] and COL.6, lines 39-49 [for the data storage within the server]; discussing each data storage facility is physically separated from any other data storage facility.

As per claim 34: See col.4, lines 13-24, discussing the authentication engine which, before the cryptographic functionality may be employed on behalf of the user, uniquely identifies the user.

As per claim 35: See COL.6, lines 28-40; discussing the plurality of data storage facilities comprises at least one secure server.

As per claim 36:

EPSTEIN teaches the method of storing authentication data in geographically remote secure data storage facilities thereby protecting the authentication data against comprise of any individual data storage facility, the method comprising:

receiving authentication data at a trust engine; **[COL.5, lines 12-14]**

combining at the trust engine the authentication data with the first substantially random value to form a first combined value; **[COL.7, lines 2-15 and 21-24]**

combining the authentication data with the second substantially random value to form a second combined value; **[COL.7, lines 18-32]**

creating a first pairing of the first substantially random value with the second combined value; **[COL.7, lines 33-38]**

creating a second pairing of the first substantially random value with the second substantially random value; **[COL.7, lines 39-43]**

storing the first pairing in a first secure data storage facility; and **[COL.7, lines 5-6]**

storing the second pairing in a second data storage facility remote from the first secure data storage facility. **[COL.7, lines 59-62]**

As per claim 37:

EPSTEIN teaches the method of storing authentication data comprising:

receiving authentication data; **[COL.5, lines 12-14]**

combining the authentication data with the first set of bits to form a second set of bits;

[COL.7, lines 2-15 and 21-24]

combining the authentication data with a third set of bits to form the fourth set of set of bits; **[COL.7, lines 18-32]**

creating a first pairing of the first set of bits with the third set of bits;

[COL.7, lines 33-38]

creating a second pairing of the first set of bits with the fourth set of bits;

[COL.7, lines 39-43]

storing one of the first and second pairing in a first computer accessible storage medium; and **[COL.7, lines 36-41]**

storing the other of the first and second pairing in a second computer accessible storage medium. **[COL.7, lines 59-62]**

As per claim 38: See COL.6, lines 39-46; discussing the first and second computer accessible storage mediums comprises at least one server.

As per claim 39: See COL.5, lines 46-66; discussing the first computer accessible storage medium is geographically remote from the second computer accessible storage medium.

As per claim 40: See COL.6, lines 14-27; discusses matching one of the first and second pairing with one of the first and second computer accessible storage medium is substantially random.

As per claim 41: See COL.5, lines 48-55; discussing the first and third set of bits are substantially random.

As per claim 42: See COL.5, lines 60-62; discussing the first and third set of bits comprises a bit length equal to a bit length of the sensitive data.

As per claim 43: See COL.6, lines 12-27; discussing the first and second pairings are needed to reassemble the data.

As per claim 44: EPSTEIN discusses creating a third pairing of the second set of bits with the third set of bits; **[COL.5, lines 42-62]** creating a fourth pairing of the second set of bits with the fourth set of bits; **[COL.6, lines 12-27]** storing one of the third and fourth pairings in a third computer accessible storage medium; and storing the other of the third and fourth pairings in a fourth computer accessible storage medium. **[COL.6, lines 39-46]**

As per claim 45:

EPSTEIN teaches the method of storing cryptographic data in geographically remote secure data storage facilities thereby protecting the cryptographic data against comprise of any individual data storage facility, the method comprising:

receiving cryptographic data at a trust engine; **[COL.5, lines 12-14]**

combining at the trust engine the cryptographic data with the first substantially random value to form a first combined value; **[COL.7, lines 2-15 and 21-24]**

combining the cryptographic data with the second substantially random value to form a second combined value; **[COL.7, lines 18-32]**

creating a first pairing of the first substantially random value with the second combined value; **[COL.7, lines 33-38]**

creating a second pairing of the first substantially random value with the second substantially random value; **[COL.7, lines 39-43]**

storing the first pairing in a first secure data storage facility; and **[COL.7, lines 5-6]**

storing the second pairing in a second data storage facility remote from the first secure data storage facility. **[COL.7, lines 59-62]**

As per claim 46:

EPSTEIN teaches the method of storing cryptographic data comprising:

receiving cryptographic data; **[COL.5, lines 12-14]**

combining the cryptographic data with the first set of bits to form a second set of bits; **[COL.7, lines 2-15 and 21-24]**

combining the cryptographic data with a third set of bits to form the fourth set of set of bits; **[COL.7, lines 18-32]**

creating a first pairing of the first set of bits with the third set of bits;
[COL.7, lines 33-38]

creating a second pairing of the first set of bits with the fourth set of bits;
[COL.7, lines 39-43]

storing one of the first and second pairings in a first computer accessible storage medium; and **[COL.7, lines 36-41]**

storing the other of the first and second pairings in a second computer accessible storage medium. **[COL.7, lines 59-62]**

As per claim 47: See COL.6, lines 39-46; discussing the first and second computer accessible storage mediums comprises at least one server.

As per claim 48: See COL.5, lines 46-66; discussing the first computer accessible storage medium is geographically remote from the second computer accessible storage medium.

As per claim 49: See COL.6, lines 14-27; discusses matching one of the first and second pairing with one of the first and second computer accessible storage medium is substantially random.

As per claim 50: See COL.5, lines 48-55; discussing the first and third set of bits are substantially random.

As per claim 51: See COL.5, lines 60-62; discussing the first and third set of bits comprises a bit length equal to a bit length of the sensitive data.

As per claim 52: See COL.6, lines 12-27; discussing the first and second pairings are needed to reassemble the data.

As per claim 53: EPSTEIN discusses creating a third pairing of the second set of bits with the third set of bits; **[COL.5, lines 42-62]** creating a fourth pairing of the second set of bits with the fourth set of bits; **[COL.6, lines 12-27]** storing one of the third and fourth pairings in a third computer accessible storage medium; and storing the other of the third and fourth pairings in a fourth computer accessible storage medium. **[COL.6, lines 39-46]**

6. Claims 59-69 are rejected under 35 U.S.C. 102(e) as being anticipated by PANG, ET AL. (US 6,446,204).

As per claim 59:

PANG discloses a secure authentication system, comprising:

a plurality of authentication engines **[FIG.8]**, wherein each authentication engine receives enrollment authentication data **[COL.1, lines 53-58 and COL.22, lines 20-22; it is inherent the enrollment data (i.e. username and password) was stored in order to reference with the current authentication data]** designed to uniquely identify a user to a degree of

certainty [COL.22, lines 36-44], each authentication engine receives current authentication data to compare to the enrollment authentication data, and wherein each authentication engine determines an authentication result; and [COL.22, lines 45-64]

a redundancy system which receives the authentication result of at least two of the authentication engines and determines whether the user has been uniquely identified. [COL.22, lines 65-67 and COL.23, lines 32-39]

As per claim 60: See COL.22, lines 50-67; discusses the redundancy system where the user has been identified by the majority of the authentication results. [The client/user sends a request for access and the plurality of providers determines whether access is authorized by sending the results if the request is authorized or authenticated. Hence, that since there includes multiple providers where each provider sends its results, it is inherent the client request is deemed authenticated by having a majority or unanimous positive results of the providers]

As per claim 61: As rejected in claim 61; discusses whether the user is uniquely identified by requiring the authentication results to be unanimously positive before issuing a positive identification.

As per claim 62:

PANG discloses a plurality of geographically remote trust engines, each trust engine having one of the plurality of authentication engines and one of the redundancy modules [FIG.8 and COL.23, lines 32-39], wherein the

redundancy module for at least one of the plurality of trust engines determines whether the user has been uniquely identified using the authentication results from ones of the authentication engines associated with the other trust engines [FIG.6 and COL.6, lines 5-19] and without using the authentication results from the at least one trust engine. [COL.22, lines 45-67]

As per claim 63: See COL.20, lines 30-54 and COL.21, lines 14-23; discussing each of the plurality of trust engines includes a depository having a computer accessible storage medium which stores a substantially randomized portion of the enrollment authentication data and wherein each depository forwards the substantially randomized portion of the enrollment authentication data to the plurality of authentication engines.

As per claim 64: See COL.20, lines 32-39 and COL.22, lines 50-67; discussing determining whether the user has been uniquely identified corresponds to the one of the redundancy modules to first determine a result.

As per claim 65:

PANG discloses a secure authentication system, comprising:

a first trust engine comprising a first depository, wherein the first depository includes a computer accessible storage medium which stores portions of enrollment authentication data; [FIG.1 and COL.5, lines 59-67]

a second trust engine located at a different geographic location than the first trust engine and comprising [COL.18, lines 6-11]

a second depository having a computer accessible storage medium which stores portions of enrollment authentication data, [COL.1, lines 53-58 and COL.22, lines 20-22; it is inherent the enrollment data (i.e. username and password) was stored in order to reference with the current authentication data]

an authentication engine communicating with the first and second depositories and which assembles at least two portions of enrollment authentication data into a usable form, and [COL.22, lines 65-67]

an transaction engine communicating with the first and second depositories and the authentication engine, [COL.5, lines 44-58 and FIG.2]

wherein the second trust engine is determined to be available to execute a transaction engine receives authentication data from the user and forwards a request for the portions of enrollment authentication data to the first and second depositories [COL.6, lines 41-50], and wherein the authentication engine receives the authentication data from the transaction engine and the portions of the enrollment authentication data from the first and second depositories, and determines an authentication result. [COL.22, lines 39-67]

As per claim 66: See FIG.2 and COL.20, lines 45-67; discussing the determination of whether the second trust engine is available to execute the transaction includes a determination of whether the second trust engine is within the geographic proximity to the user.

As per claim 67: See COL.10, lines 31-51 and COL.23, lines 10-20; discusses determining of whether the second trust engine is available to execute the transaction includes a determination of whether the second trust engine is currently servicing a light system load.

As per claim 68: See COL.25, lines 30-38; discusses determining of whether the second trust engine is currently scheduled for maintenance.

As per claim 69: See COL.22, lines 39-67, discusses the first and second trust engines are determined to be available, and an authentication result for the trust engine system follows the first and second trust engines to produce the authentication result.

Response to Arguments

7. Applicant's arguments filed September 9, 2004 have been fully considered but they are not persuasive.

Borza

A.) In response to applicant's arguments, the recitation "**a remotely accessible secure cryptographic system**" has not been given patentable weight because the recitation occurs in the preamble. A preamble is generally

not accorded any patentable weight where it merely recites the purpose of a process or the intended use of a structure, and where the body of the claim does not depend on the preamble for completeness but, instead, the process steps or structural limitations are able to stand alone. See *In re Hirao*, 535 F.2d 67, 190 USPQ 15 (CCPA 1976) and *Kropa v. Robie*, 187 F.2d 150, 152, 88 USPQ 478, 481 (CCPA 1951).

Borza discloses the fingerprint received from the imaging device and the algorithm specific (of the encryption/decryption circuit 124) for generating data from the image is the randomized data (COL.7, lines 30-38 and COL.8, lines 48-51). The encryption process has to be random in order to be secure to be unreadable to unauthorized individuals, else, encryption is not needed.

Epstein

Epstein discloses having a private/public key pair (col.4, lines 24-36) where storing either the private or the public key at the server is inherent and that is not a patentable distinction.

B.) In response to applicant's argument that ***storing the private key on a secure server***, a recitation of the intended use of the claimed invention must result in a structural difference between the claimed invention and the prior art in order to patentably distinguish the claimed invention from the prior art. If the prior art structure is capable of performing the intended use, then it meets the claim. In a claim drawn to a process of making, the intended use must

result in a manipulative difference as compared to the prior art. See *In re Casey*, 370 F.2d 576, 152 USPQ 235 (CCPA 1967) and *In re Otto*, 312 F.2d 937, 939, 136 USPQ 458, 459 (CCPA 1963).

The “data splitting module” and “data assembling module” is where the authentication data such as passwords, biometric data, user ID, and keys is received and created into portions that is stored at storage facilities to assemble into authentication data (col.4, lines 54-58 and col.5, lines 63-66) for latter use for comparison purposes.

Pang

Pang includes plurality of authentication engines (col.23, lines 32-33) and a second trust engine located at a different geographic location than the first trust engine (COL.17, line 48-col.8, lines 11)

Conclusion

8. THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the

advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to LEYNNA T. HA whose telephone number is (571) 272-3851. The examiner can normally be reached on Monday - Thursday (7:00 - 5:00PM).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

LHa


KIM VU
SPECIALIST PATENT EXAMINER
TECHNOLOGY CENTER 2100